Advanced Portal Security (APS)

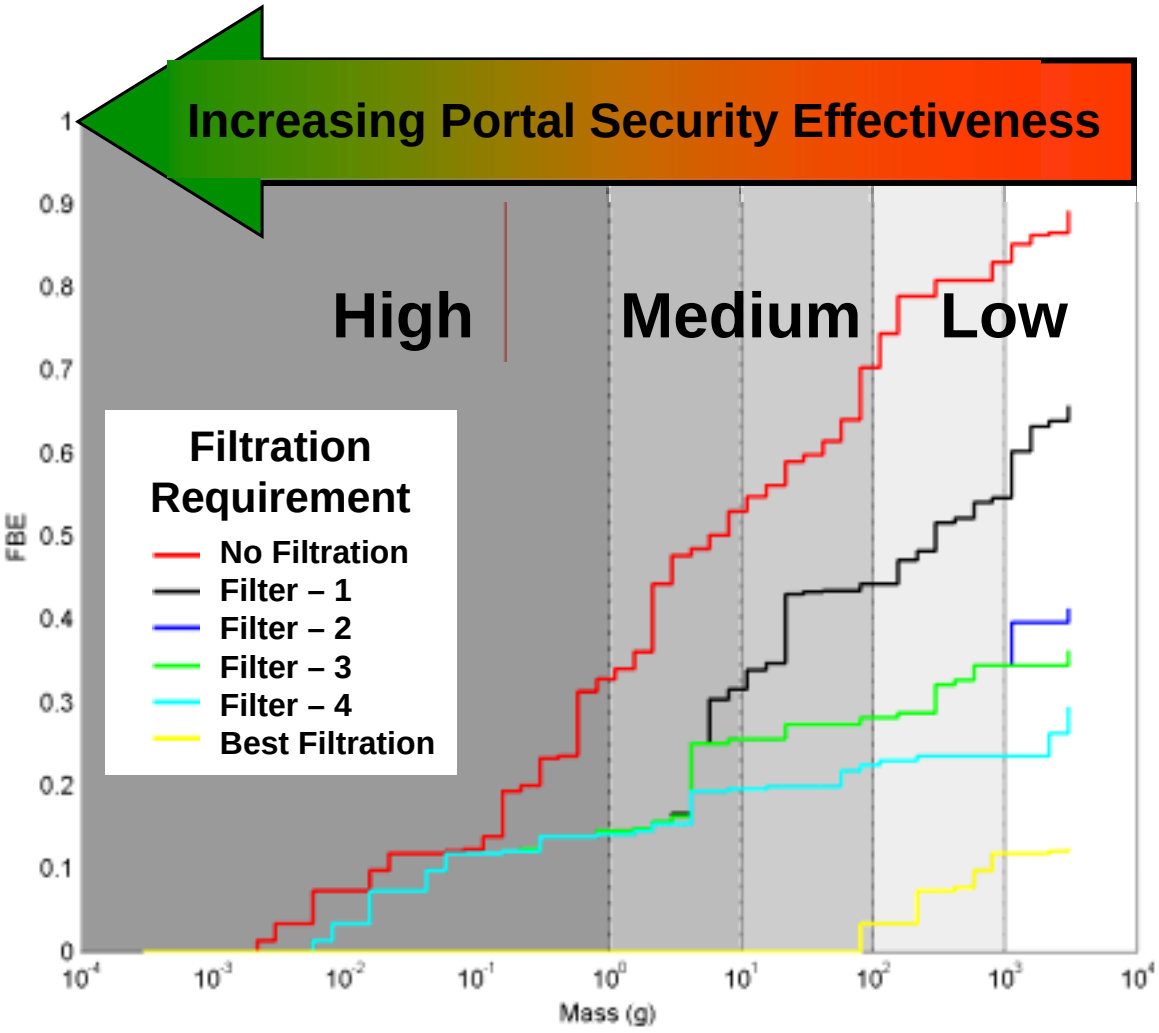
Wayne Bryden
Program Manager
Special Projects Office
Defense Advanced Research Projects Agency

Advanced Portal Security Program

- **Threat:** An unconventional attack against military/civilian buildings and bases with chemical or biological agents
  - Threat agent hidden in a sealed container and carried into a building resulting in an internal release
- **Goal:** Make buildings and bases safer from CW/BW attack
  - Reduce the risk of an internal release by detecting chemical and biological agents prior to entry

Relationship between Portal Security and Fraction of Building Exposed

Notional Internal Release Scenario



FBE can be reduced by improving portal security or the protection architecture

Portal security:

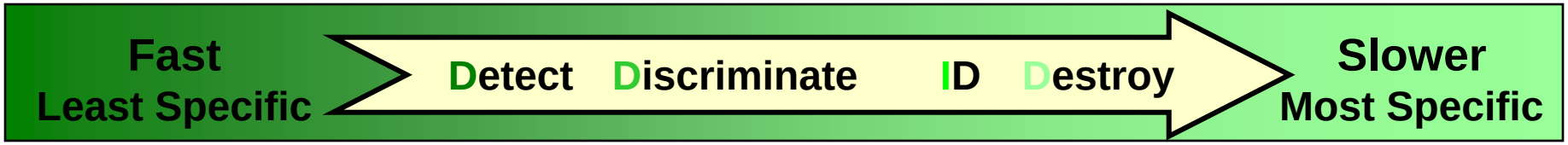
- **Can reduce the range of potential masses**
- **Does not eliminate the threat**
- **Enables performance tradeoffs to achieve detection of low quantities:**
  - **Mass**
  - **Scan Time**
  - **Pd/Pfa**
  - **Specificity**

Portal Security Applications

Approach: Develop family of screening technologies for the following "applications"

- Front Lobby
  - People, Packages, Containers, and Single Items
  - Find small quantities of CW/BW agents
    - Detect small objects hidden under clothing and protect personal privacy
    - Verify contents of packages and containers
- Mailroom
  - Normal Business Mail, Flats, Packages, Containers
  - Find small quantities of CW/BW agents
    - Protect against known threats
    - Reduce logistics burden

Multi-Level Screening Concepts



Threat Space

Bags – bottle hidden in a bag, briefcase, etc.

Bottles – closed, sealed containers of liquid or powder material.

Mail – envelopes (single or in bundles).

People – bottle or other container hidden under clothing.

Conceptual Process

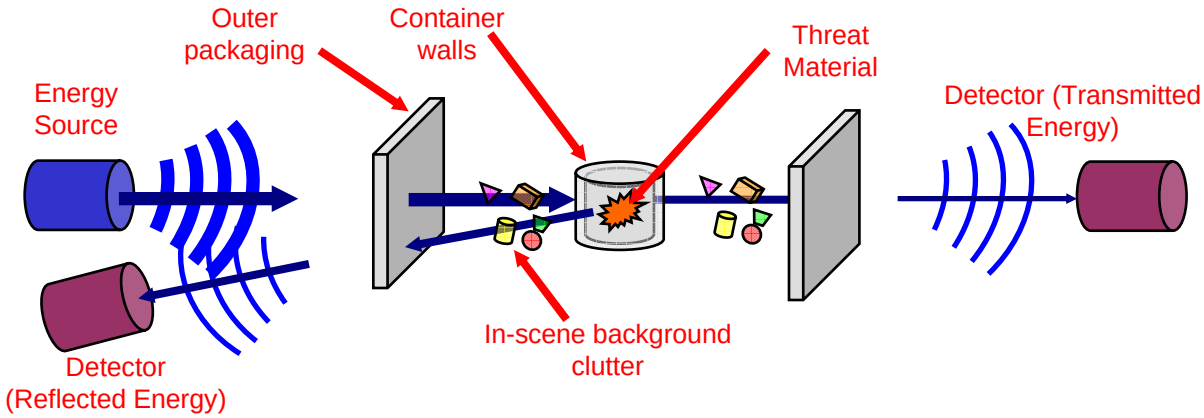
1. Anomaly Detection. First level screening to detect anomalies and potential threat containers hidden in a bag, or inside another container, or under clothing.

2. Hazard Discrimination. Second level screening to distinguish between hazardous and benign substances inside containers based on physical and chemical properties of liquids, solids and biological materials.

3. Threat Identification. Third level screening to identify threat materials from the chemical composition of spectroscopic signature.

4. Threat Destruction. Energy tailored to destroy CB agents without collateral damage to non-hazardous items.

Generic Screening Concept



Common Schema

The easiest case is the **stand-alone bottle** with no other packaging or background clutter.

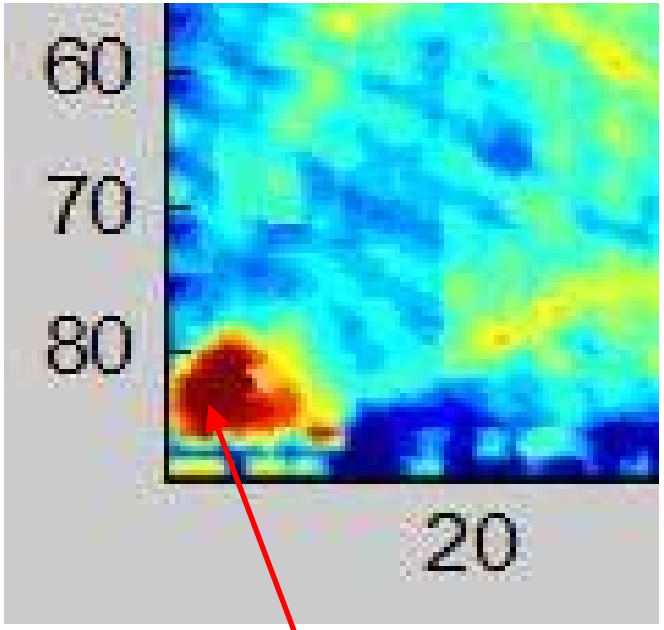
A **suitcase** has an *outer packaging* (the suitcase) and other internal *background clutter* (clothes, personal items, etc.).

Mail has an *outer packaging* (the envelope) and other internal *background clutter* (paper, metal staples, etc.).

People have *outer packaging* (their clothes) and other internal *background clutter* (jewelry, belts, pens, wallets, cell phones, etc.).

Mail (Letters & Flats) Screening

- Desired Capabilities
  - Automated scan to detect & discriminate powders prior to opening
  - Fast trigger scan
    - Duration: < few seconds
    - Detection: < small quantities of powder
  - Confirmation scan
    - Duration: few seconds
    - Discriminate detected material as possible threat or hoax

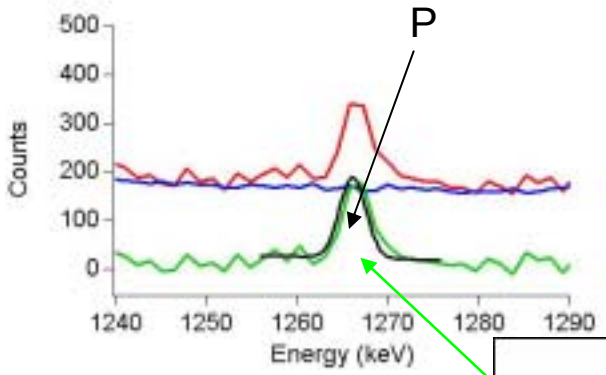


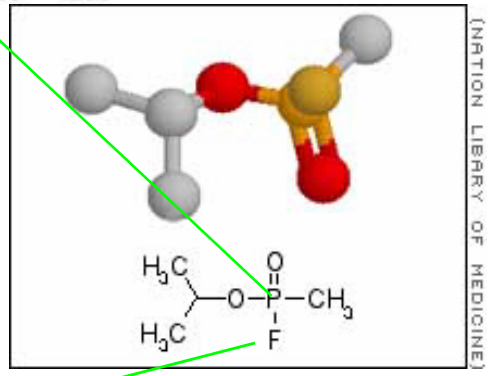
Detection of
powder samples
inside standard envelopes
at a single NIR wavelength
after corner concentration
Scan time ~ seconds/image

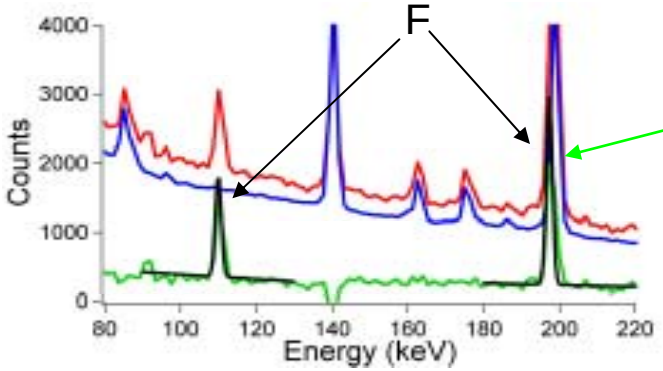
Package Screening

- Desired Capabilities
  - Scan for CW/TICs prior to opening
  - Fast trigger scan
    - 5 per minute for lobby
    - 1 per minute for mailroom
  - Confirmation scan
    - High Pd
    - Low Pfa
  - Complements X-ray & explosives detection systems
  - No safety issues
  - Uses limited floor space

Possible Sarin detection by discrimination of fluorine and phosphorus

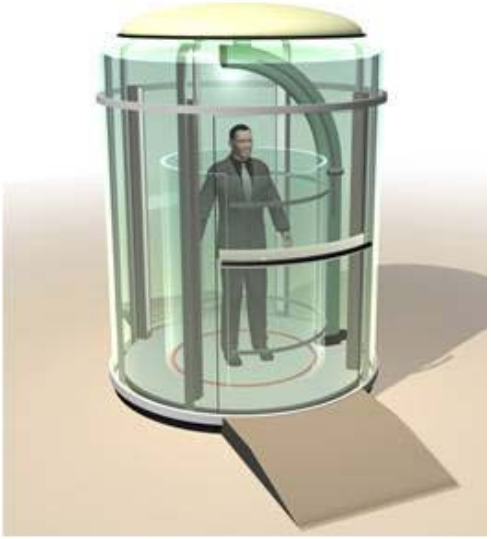




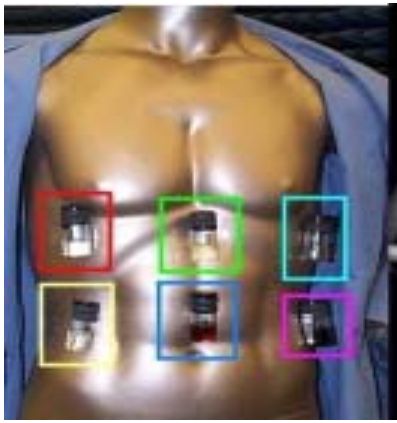


Personnel Screening

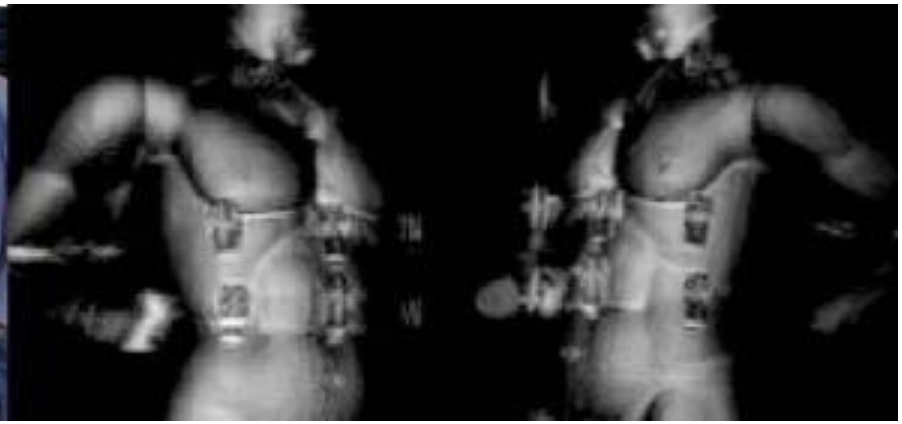
- Desired Capabilities
  - 3D scanning of ~10 people per minute
  - Detect liquids
  - Detect powders
  - Detect glass & plastic containers; paper envelopes; plastic bags
  - No safety or privacy issues
  - Use limited floor space



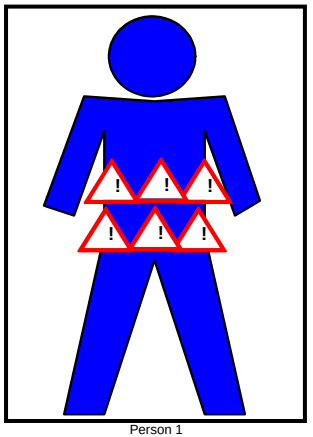
Optical Image



22-33 GHz Images



Desired Operator Image



Program Approach

- Phase I: Technology Assessment (FY02)
  - BAA solicitation of industry/OGAs. Independent investigations.
  - >50 responses - identified viable technologies
  - Technology Feasibility Studies (FY02-03)
    - Research contracts awarded
    - Demonstrated qualitative evidence of penetration & signatures
- Phase II: Technology Development (FY05-06)
  - Develop and optimize selected technologies to quantify/enhance performance
  - Invest in prototype development efforts to ensure successful transition of those technologies
    - Achieve integrated mail system prototype
    - Achieve personal screening prototype
- Phase III: System Demonstration (FY07-08)
  - Integrate complementary technologies to demo performance